Release Notes for the Catalyst 2960-S Switches, Cisco IOS Release 12.2(53)SE1

Updated April 9, 2010

Cisco IOS Release 12.2(53)SE1 runs on Catalyst 2960-S switches.

Some models of the switches support Cisco FlexStack and are stacking-capable. Unless otherwise noted, the term *switch* refers to a standalone switch and to a switch stack.

These release notes include important information about Cisco IOS Release 12.2(53)SE1 and any limitations, restrictions, and caveats that apply to the releases. Verify that these release notes are correct for your switch:

- If you are installing a new switch, see the Cisco IOS release label on the rear panel of your switch.
- If your switch is on, use the **show version** privileged EXEC command. See the "Finding the Software Version and Feature Set" section on page 5.

For the complete list of Catalyst 2960-S switch documentation, see the "Related Documentation" section on page 18.

You can download the switch software from this site (registered Cisco.com users with a login password):

http://www.cisco.com/cisco/web/download/index.html

Contents

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

System Requirements

Supported Hardware

Table 1 Catalyst 2960-S Switches

Hardware	Description	Supported by Minimum Cisco IOS Release
Catalyst 2960S-48FPD-L[1]	48 10/100/1000 Power over Ethernet Plus (PoE+) ports (PoE budget of 740 W) and 2 small form-factor pluggable (SFP)+[2] module slots	Cisco IOS Release 12.2(53)SE1
Catalyst 2960S-48LPD-L[1]	48 10/100/1000 PoE+ ports (PoE budget of 370 W) and 2 SFP+ module slots	Cisco IOS Release 12.2(53)SE1
Catalyst 2960S-24PD-L[1]	24 10/100/1000 PoE+ ports (PoE budget of 370 W) and 2 SFP+ module slots	Cisco IOS Release 12.2(53)SE1
Catalyst 2960S-48TD-L[1]	48 10/100/1000 ports and 2 SFP+ module slots	Cisco IOS Release 12.2(53)SE1
Catalyst 2960S-24TD-L[1]	24 10/100/1000 ports and 2 SFP+ module slots	Cisco IOS Release 12.2(53)SE1
Catalyst 2960S-48FPS-L[1]	48 10/100/1000 PoE+ ports (PoE budget of 740 W) and 4 SFP[3] module slots	Cisco IOS Release 12.2(53)SE1
Catalyst 2960S-48LPS-L[1]	48 10/100/1000 PoE+ ports (PoE budget of 370 W) and 4 SFP module slots	Cisco IOS Release 12.2(53)SE1
Catalyst 2960S-24PS-L[1]	24 10/100/1000 PoE+ ports (PoE budget of 370 W) and 4 SFP module slots	Cisco IOS Release 12.2(53)SE1
Catalyst 2960S-48TS-L[1]	48 10/100/1000 ports and 4 SFP module slots	Cisco IOS Release 12.2(53)SE1
Catalyst 2960S-24TS-L[1]	24 10/100/1000 ports and 4 SFP module slots	Cisco IOS Release 12.2(53)SE1
Catalyst 2960S-48TS-S	48 10/100/1000 ports and 2 SFP module slots	Cisco IOS Release 12.2(53)SE1
Catalyst 2960S-24TS-S	24 10/100/1000 ports and 2 SFP module slots	Cisco IOS Release 12.2(53)SE1

1.Support Cisco FlexStack technology.

2.SFP+ = 10 Gigabit fiber uplink.

3.SFP = 1 Gigabit fiber uplink.

Table 2 Supported Power Supply

Hardware	Description	Supported by Minimum Cisco IOS Release
Redundant power systems	Cisco Redundant Power System 2300	Cisco IOS Release 12.2(53)SE1

Table 3 Supported SFP and SFP+ Modules

SFP Transceiver	Description	Catalyst 2960-S D-L Switches	Catalyst 2960-S S-L Switches	Catalyst 2960-S S-S Switches
GLC-BX-D=	1000BASE-BX SFP, 1490NM	Yes	Yes	No
GLC-BX-U=	1000BASE-BX SFP, 1310NM	Yes	Yes	No
GLC-FE-100BX-D=	100BASE-BX SFP, 1490NM	No	Yes	No
GLC-FE-100BX-U=	100BASE-BX SFP, 1310NM	No	Yes	No
GLC-GE-100FX=	100BASE-FX SFP for GE SFP port	No	Yes	Yes
GLC-FE-100FX=	100BASE-FX SFP for FE SFP port	No	Yes	Yes
GLC-FE-100LX=	100BASE-LX SFP	No	Yes	No
GLC-LH-SM=	GE SFP, LC connector LX/LH transceiver	Yes	Yes	Yes
GLC-SX-MM=	GE SFP, LC connector SX transceiver	Yes	Yes	Yes
GLC-ZX-SM=	1000BASE-ZX SFP	Yes	Yes	Yes
CWDM-SFP-1470=	CWDM 1470 NM SFP Gigabit Ethernet and 1G/2G FC	Yes	Yes	No
CWDM-SFP-1490=	CWDM 1490 NM SFP Gigabit Ethernet and 1G/2G FC	Yes	Yes	No
CWDM-SFP-1510=	CWDM 1510 NM SFP Gigabit Ethernet and 1G/2G FC	Yes	Yes	No
CWDM-SFP-1530=	CWDM 1530 NM SFP Gigabit Ethernet and 1G/2G FC	Yes	Yes	No
CWDM-SFP-1550=	CWDM 1550 NM SFP Gigabit Ethernet and 1G/2G FC	Yes	Yes	No
CWDM-SFP-1570=	CWDM 1570 NM SFP Gigabit Ethernet and 1G/2G FC	Yes	Yes	No
CWDM-SFP-1590=	CWDM 1590 NM SFP Gigabit Ethernet and 1G/2G FC	Yes	Yes	No
CWDM-SFP-1610=	CWDM 1610 NM SFP Gigabit Ethernet and 1G/2G FC	Yes	Yes	No
SFP-10G-LR=	10GBASE-LR SFP+ Module	Yes	No	No
SFP-10G-SR=	10GBASE-SR SFP+ Module	Yes	No	No
SFP-10G-LRM=	10GBASE-LRM SFP+ Module	Yes	No	No

Table 3 Supported SFP and SFP+ Modules (continued)

SFP Transceiver	Description	Catalyst 2960-S D-L Switches	Catalyst 2960-S S-L Switches	Catalyst 2960-S S-S Switches
SFP-H10GB-CU1M	10GBASE-CU SFP+ Cable 1 Meter	Yes	No	No
SFP-H10GB-CU3M	10GBASE-CU SFP+ Cable 3 Meter	Yes	No	No
SFP-H10GB-CU5M	10GBASE-CU SFP+ Cable 5 Meter	Yes	No	No

Device Manager System Requirements

Hardware Requirements

Table 4 Minimum Hardware Requirements

Processor Speed	DRAM	Number of Colors	Resolution	Font Size
233 MHz minimum[1]	512 MB[2]	256	1024 x 768	Small

1. We recommend 1 GHz.
2. We recommend 1 GB DRAM.

Software Requirements

These are the supported operating systems and browsers for the device manager:

- Windows 2000, XP, Vista, and Windows Server 2003.
- Internet Explorer 5.5, 6.0, 7.0, Firefox 1.5, 2.0 or later.

The device manager verifies the browser version when starting a session, and it does not require a plug-in.

CNA Compatibility

Cisco IOS 12.2(53)SE1 will be supported in a future release of the Cisco Network Assistant. You can download Cisco Network Assistant from this URL:

http://www.cisco.com/pcgi-bin/tablebuild.pl/NetworkAssistant

For more information about Cisco Network Assistant, see the *Release Notes for Cisco Network Assistant* on Cisco.com.

Upgrading the Switch Software

These are the procedures for downloading software. Before downloading software, read this section for important information:

Finding the Software Version and Feature Set

The Cisco IOS image is stored as a bin file in a directory that is named with the Cisco IOS release. A subdirectory contains the files needed for web management. The image is stored on the system board flash device (flash:).

You can use the **show version** privileged EXEC command to see the software version that is running on your switch. The second line of the display shows the version.

You can also use the **dir** *filesystem***:** privileged EXEC command to see the directory names of other software images that you might have stored in flash memory.

Deciding Which Files to Use

The upgrade procedures in these release notes describe how to perform the upgrade by using a combined tar file. This file contains the Cisco IOS image file and the files needed for the embedded device manager. You must use the combined tar file to upgrade the switch through the device manager. To upgrade the switch through the command-line interface (CLI), use the tar file and the **archive download-sw** privileged EXEC command.

Table 5 Cisco IOS Software Tar File

Filename	Description
c2960s-universalk9-tar.122-53.SE1.tar	Catalyst 2960-S image file and device manager files.

The switch image file contains two feature sets: LAN lite and LAN base.

Switches with model numbers that have a *-S* in the product ID, such as Catalyst 2960S-48TS-S, support the LAN lite feature set. This feature set does not support stacking. These switches have a metal cover over the stack module slot to prevent a stack module from being installed. These switches support the LAN lite SDM template.

Switches with model numbers that have a *-L* in the product ID, such as Catalyst 2960S-24TS-L, support the LAN base feature set. These switches support the FlexStack modules and the LAN base SDM template.

You can use the **show version** privileged EXEC command to display the running image.

Archiving Software Images

Before upgrading your switch software, make sure that you have archived copies of the current Cisco IOS release and the Cisco IOS release to which you are upgrading. You should keep these archived images until you have upgraded all devices in the network to the new Cisco IOS image and until you have verified that the new Cisco IOS image works properly in your network.

Cisco routinely removes old Cisco IOS versions from Cisco.com. See *Product Bulletin 2863* for more information:

http://www.cisco.com/en/US/prod/collateral/iosswrel/ps8802/ps6969/ps1835/prod_bulletin0900aecd80281c0e.html

You can copy the bin software image file on the flash memory to the appropriate TFTP directory on a host by using the **copy flash: tftp:** privileged EXEC command.

Note Although you can copy any file on the flash memory to the TFTP server, it is time consuming to copy all of the HTML files in the tar file. We recommend that you download the tar file from Cisco.com and archive it on an internal host in your network.

You can also configure the switch as a TFTP server to copy files from one switch to another without using an external TFTP server by using the **tftp-server** global configuration command. For more information about the **tftp-server** command, see the "Basic File Transfer Services Commands" section of the *Cisco IOS Configuration Fundamentals Command Reference, Release 12.2* at this URL:

http://www.cisco.com/en/US/docs/ios/12_2/configfun/command/reference/ffun_r.html

Upgrading a Switch by Using the Device Manager or Network Assistant

You can upgrade switch software by using the device manager or Network Assistant. For detailed instructions, click **Help**.

Note When using the device manager to upgrade your switch, do not use or close your browser session after the upgrade process begins. Wait until after the upgrade process completes.

Upgrading a Switch by Using the CLI

This procedure is for copying the combined tar file to the switch. You copy the file to the switch from a TFTP server and extract the files. You can download an image file and replace or keep the current image.

To download software, follow these steps:

Step 1 Log in and download the software image file:

http://tools.cisco.com/support/downloads/go/Redirect.x?mdfid=268438038

To download the image for a Catalyst 2960-S switch, click **Catalyst 2960-S software**.

Step 2 Copy the image to the appropriate TFTP directory on the workstation, and make sure that the TFTP server is properly configured.

For more information, see Appendix B in the software configuration guide for this release.

Step 3 Log into the switch through the console port or a Telnet session.

Step 4 (Optional) Ensure that you have IP connectivity to the TFTP server by entering this privileged EXEC command:

```
Switch# ping tftp-server-address
```

For more information about assigning an IP address and default gateway to the switch, see the software configuration guide for this release.

Step 5 Download the image file from the TFTP server to the switch. If you are installing the same version of software that is currently on the switch, overwrite the current image by entering this privileged EXEC command:

```
Switch# archive download-sw /overwrite /reload
tftp:[[//location]/directory]/image-name.tar
```

The **/overwrite** option overwrites the software image in flash memory with the downloaded one.

The **/reload** option reloads the system after downloading the image unless the configuration has been changed and not saved.

For **//***location*, specify the IP address of the TFTP server.

For */directory*/*image-name*.**tar**, specify the directory (optional) and the image to download. Directory and image names are case sensitive.

This example shows how to download an image from a TFTP server at 198.30.20.19 and to overwrite the image on the switch:

```
Switch# archive download-sw /overwrite
tftp://198.30.20.19/c2960s-universalk9-tar.122-50.SE.tar
```

You can also download the image file from the TFTP server to the switch and keep the current image by replacing the **/overwrite** option with the **/leave-old-sw** option.

Recovering from a Software Failure

For additional recovery procedures, see the “Troubleshooting” chapter in the software configuration guide for this release.

Installation Notes

You can assign IP information to your switch by using these methods:

- The Express Setup program, as described in the switch getting started guide.
- The CLI-based setup program, as described in the switch hardware installation guide.
- The DHCP-based autoconfiguration or Smart Install feature, as described in the switch software configuration guide
- Manually assigning an IP address, as described in the switch software configuration guide.

New Features

New Hardware Features

For a list of all supported hardware, see the Supported Hardware, page 2.

New Software Features

This release is the first software release for the Catalyst 2960-S switches. For a detailed list of key features for this software release, see the *Catalyst 2960 and 2960-S Switch Software Configuration Guide*.

Table 6 lists the software features that are supported only on the Catalyst 2960-S switches. These features are not supported on the Catalyst 2960 switches.

Table 6 Catalyst 2960-S Switch Features Specific to Only the Catalyst 2960-S Switches

Feature	Minimum Cisco IOS Release Required	Catalyst Switch Support
Online diagnostics to test the functionality of the supervisor engine, modules, and switch.	12.2(53)SE1	2960-S
On-board failure logging (OBFL) to collect information about the switch and any connected power supplies.	12.2(53)SE1	2960-S
SFP+ support for 10 Gigabit.	12.2(53)SE1	2960-S
Cisco FlexStack technology (available in the LAN base feature set): • Supports stacking up to four switches through their FlexStack ports to operate as a single switch in the network. • Supports a bidirectional 20-Gb/s switching fabric across the switch stack, with all stack members having full access to the system bandwidth. • Uses a single IP address and configuration file to manage the entire switch stack. • Supports automatic Cisco IOS version-check of new stack members with the option to automatically load images from the stack's active switch or from a TFTP server. • Supports adding, removing, and replacing of switches in the stack without disrupting the operation of the stack.	12.2(53)SE1	2960-S
IEEE 802.3at, the PoE+ standard that increases the maximum power that can be drawn by a powered device from 15.4 W per port to 30 W per port.	12.2(53)SE1	2960-S

Table 6 Catalyst 2960-S Switch Features Specific to Only the Catalyst 2960-S Switches (continued)

Feature	Minimum Cisco IOS Release Required	Catalyst Switch Support
USB mini-Type B console connection and RJ-45 console connection. Only one console connection can be active at a time.	12.2(53)SE1	2960-S
USB Type A port for access to external USB flash memory (thumb drives or USB keys).	12.2(53)SE1	2960-S

Limitations and Restrictions

You should review this section before you begin working with the switch. These are known limitations that will not be fixed, and there is not always a workaround. Some features might not work as documented, and some features could be affected by recent changes to the switch hardware or software.

This section contains these limitations:

- Cisco IOS Limitations, page 9
- Device Manager Limitations, page 14

Cisco IOS Limitations

- Configuration Limitations, page 10
- Ethernet Limitations, page 11
- HSRP Limitations, page 11
- IP Limitations, page 11
- IP Telephony Limitations, page 12
- Multicasting Limitations, page 12
- PoE+ Limitations, page 13
- Quality of Service Limitations, page 13
- RADIUS Limitations, page 13
- SPAN and Remote SPAN Limitations, page 13
- Trunking Limitations, page 14
- VLAN Limitations, page 14

Configuration Limitations

- A static IP address might be removed when the previously acquired DHCP IP address lease expires.

  This problem occurs under these conditions:

  - When the switch is booted up without a configuration (no config.text file in flash memory).
  - When the switch is connected to a DHCP server that is configured to give an address to it (the dynamic IP address is assigned to VLAN 1).
  - When an IP address is configured on VLAN 1 before the dynamic address lease assigned to VLAN 1 expires.

  The workaround is to reconfigure the static IP address. (CSCea71176 and CSCdz11708)

- When connected to some third-party devices that send early preambles, a switch port operating at 100 Mb/s full duplex or 100 Mb/s half duplex might bounce the line protocol up and down. The problem is observed only when the switch is receiving frames.

  The workaround is to configure the port for 10 Mb/s and half duplex or to connect a hub or a nonaffected device to the switch. (CSCed39091)

- When port security is enabled on an interface in restricted mode and the **switchport block unicast interface** command has been entered on that interface, MAC addresses are incorrectly forwarded when they should be blocked.

  The workaround is to enter the **no switchport block unicast** interface configuration command on that specific interface. (CSCee93822)

- When the **logging event-spanning-tree** interface configuration command is configured and logging to the console is enabled, a topology change might generate a large number of logging messages, causing high CPU utilization. CPU utilization can increase with the number of spanning-tree instances and the number of interfaces configured with the **logging event-spanning-tree** interface configuration command. This condition adversely affects how the switch operates and could cause problems such as STP convergence delay.

  High CPU utilization can also occur with other conditions, such as when debug messages are logged at a high rate to the console.

  Use one of these workarounds:

  - Disable logging to the console.
  - Rate-limit logging messages to the console.
  - Remove the **logging event spanning-tree** interface configuration command from the interfaces. (CSCsg91027)

- The far-end fault optional facility is not supported on the GLC-GE-100FX SFP module.

  The workaround is to configure aggressive UDLD. (CSCsh70244).

- When you enter the **boot host retry timeout** global configuration command to specify the amount of time that the client should keep trying to download the configuration and you do not enter a timeout value, the default value is zero, which should mean that the client keeps trying indefinitely. However, the client does not keep trying to download the configuration.

  The workaround is to always enter a non zero value for the timeout value when you enter the **boot host retry timeout** *timeout-value* command. (CSCsk65142)

- A ciscoFlashMIBTrap message appears during switch startup. This does not affect switch functionality. (CSCsj46992)
- If you enter the **show tech-support** privileged EXEC command after you enter the **remote command** {**all** | *stack-member-number*} privileged EXEC command, the complete output does not appear.

  The workaround is to use the **session** *stack-member-number* privileged EXEC command. (CSCsz38090)

Ethernet Limitations

- Traffic on EtherChannel ports is not perfectly load-balanced. Egress traffic on EtherChannel ports are distributed to member ports on load balance configuration and traffic characteristics like MAC or IP address. More than one traffic stream may map to same member ports based on hashing results calculated by the ASIC.

  If this happens, uneven traffic distribution will happen on EtherChannel ports.

  Changing the load balance distribution method or changing the number of ports in the EtherChannel can resolve this problem. Use any of these workarounds to improve EtherChannel load balancing:

  – for random source-ip and dest-ip traffic, configure load balance method as **src-dst-ip**

  – for incrementing source-ip traffic, configure load balance method as **src-ip**

  – for incrementing dest-ip traffic, configure load balance method as **dst-ip**

  – Configure the number of ports in the EtherChannel so that the number is equal to a power of 2 (i.e. 2, 4, or 8)

  For example, with load balance configured as **dst-ip** with 150 distinct incrementing destination IP addresses, and the number of ports in the EtherChannel set to either 2, 4, or 8, load distribution is optimal.(CSCeh81991)

HSRP Limitations

- When the active switch fails in a switch cluster that uses Hot Standby Routing Protocol (HSRP) redundancy, the new active switch might not contain a full cluster member list. The workaround is to ensure that the ports on the standby cluster members are not in the spanning-tree blocking state. To verify that these ports are not in the blocking state, see the “Configuring STP” chapter in the software configuration guide. (CSCec76893)

IP Limitations

- When the rate of received DHCP requests exceeds 2,000 packets per minute for a long time, the response time might be slow when you are using the console. The workaround is to use rate limiting on DHCP traffic to prevent a denial of service attack from occurring. (CSCeb59166)

IP Telephony Limitations

- After you change the access VLAN on a port that has IEEE 802.1x enabled, the IP phone address is removed. Because learning is restricted on IEEE 802.1x-capable ports, it takes approximately 30 seconds before the address is relearned. No workaround is necessary. (CSCea85312)
- Some access point devices are incorrectly discovered as IEEE 802.3af Class 1 devices. These access points should be discovered as Cisco pre-standard devices. The **show power inline** user EXEC command shows the access point as an IEEE Class 1 device. The workaround is to power the access point by using an AC wall adaptor. (CSCin69533)
- The Cisco 7905 IP Phone is error-disabled when the phone is connected to wall power.

  The workaround is to enable PoE and to configure the switch to recover from the PoE error-disabled state. (CSCsf32300)

Multicasting Limitations

- If the number of multicast routes and Internet Group Management Protocol (IGMP) groups are more than the maximum number specified by the **show sdm prefer** global configuration command, the traffic received on unknown groups is flooded in the received VLAN even though the **show ip igmp snooping multicast-table** privileged EXEC command output shows otherwise. The workaround is to reduce the number of multicast routes and IGMP snooping groups to less than the maximum supported value. (CSCdy09008)
- IGMP filtering is applied to packets that are forwarded through hardware. It is not applied to packets that are forwarded through software. Hence, with multicast routing enabled, the first few packets are sent from a port even when IGMP filtering is set to deny those groups on that port. There is no workaround. (CSCdy82818)
- If an IG MP report packet has two multicast group records, the switch removes or adds interfaces depending on the order of the records in the packet:
  - If the ALLOW_NEW_SOURCE record is before the BLOCK_OLD_SOURCE record, the switch removes the port from the group.
  - If the BLOCK_OLD_SOURCE record is before the ALLOW_NEW_SOURCE record, the switch adds the port to the group.

  There is no workaround. (CSCec20128)
- When IGMP snooping is disabled and you enter the **switchport block multicast** interface configuration command, IP multicast traffic is not blocked.

  The **switchport block multicast** interface configuration command is only applicable to non-IP multicast traffic.

  There is no workaround. (CSCee16865)
- Incomplete multicast traffic can be seen under either of these conditions:
  - You disable IP multicast routing or re-enable it globally on an interface.
  - A switch mroute table temporarily runs out of resources and recovers later.

  The workaround is to enter the **clear ip mroute** privileged EXEC command on the interface. (CSCef42436)

  After you configure a switch to join a multicast group by entering the **ip igmp join-group** *group-address* interface configuration command, the switch does not receive join packets from the client, and the switch port connected to the client is removed from the IGMP snooping forwarding table.

Use one of these workarounds:

- Cancel membership in the multicast group by using the **no ip igmp join-group** *group-address* interface configuration command on an SVI.
- Disable IGMP snooping on the VLAN interface by using the **no ip igmp snooping vlan** *vlan-id* global configuration command. (CSCeh90425)

- A switch drops unicast traffic under these conditions:
  - The switch belongs to a Layer 2 ring.
  - More than 800 Mbps of multicast traffic is sent in both directions on the interface.

  When multicast traffic is sent in one direction and unicast traffic is sent in another, unicast traffic is dropped at the multicast traffic source port.

  The workaround is to apply a policy map so that the least significant traffic is discarded. (CSCsq83882)

PoE+ Limitations

- When a powered device (such as an IP phone) connected to a PoE+ port restarts and sends a CDP or LLDP packet with a power TLV, the switch locks to the power-negotiation protocol of that first packet. The switch does not respond to power requests from the other protocol. For example, if the switch is locked to CDP, it does not provide power to devices that send LLDP requests. If CDP is disabled after the switch has locked on it, the switch does not respond to LLDP power requests and can no longer power on any accessories.

  The workaround is to turn the powered device off and then on again.

Quality of Service Limitations

- Some switch queues are disabled if the buffer size or threshold level is set too low with the **mls qos queue-set output** global configuration command. The ratio of buffer size to threshold level should be greater than 10 to avoid disabling the queue. The workaround is to choose compatible buffer sizes and threshold levels. (CSCea76893)
- When auto-QoS is enabled on the switch, priority queuing is not enabled. Instead, the switch uses shaped round robin (SRR) as the queuing mechanism. The auto-QoS feature is designed on each platform based on the feature set and hardware limitations, and the queuing mechanism supported on each platform might be different. There is no workaround. (CSCee22591)

RADIUS Limitations

- RADIUS change of authorization (COA) reauthorization is not supported on the critical auth VLAN.

  There is no workaround. (CSCta05071)

SPAN and Remote SPAN Limitations

- Cisco Discovery Protocol (CDP), VLAN Trunking Protocol (VTP), and Port Aggregation Protocol (PAgP) packets received from a SPAN source are not sent to the destination interfaces of a local SPAN session. The workaround is to use the **monitor session** *session_number* **destination** {**interface** *interface-id* **encapsulation replicate**} global configuration command for local SPAN. (CSCed24036)

Trunking Limitations

- The switch treats frames received with mixed encapsulation (IEEE 802.1Q and Inter-Switch Link [ISL]) as frames with FCS errors, increments the error counters, and the port LED blinks amber. This happens when an ISL-unaware device receives an ISL-encapsulated packet and forwards the frame to an IEEE 802.1Q trunk interface. There is no workaround. (CSCdz33708)
- IP traffic with IP options set is sometimes leaked on a trunk port. For example, a trunk port is a member of an IP multicast group in VLAN X but is not a member in VLAN Y. If VLAN Y is the output interface for the multicast route entry assigned to the multicast group and an interface in VLAN Y belongs to the same multicast group, the IP-option traffic received on an input VLAN interface other than one in VLAN Y is sent on the trunk port in VLAN Y because the trunk port is forwarding in VLAN Y, even though the port has no group membership in VLAN Y. There is no workaround. (CSCdz42909).
- For trunk ports or access ports configured with IEEE 802.1Q tagging, inconsistent statistics might appear in the **show interfaces counters** privileged EXEC command output. Valid IEEE 802.1Q frames of 64 to 66 bytes are correctly forwarded even though the port LED blinks amber, and the frames are not counted on the interface statistics. There is no workaround. (CSCec35100).

VLAN Limitations

- If the number of VLANs times the number of trunk ports exceeds the recommended limit of 13,000, the switch can fail.

  The workaround is to reduce the number of VLANs or trunks. (CSCeb31087)
- When line rate traffic is passing through a dynamic port, and you enter the **switchport access vlan dynamic** interface configuration command for a range of ports, the VLANs might not be assigned correctly. One or more VLANs with a null ID appears in the MAC address table instead.

  The workaround is to enter the **switchport access vlan dynamic** interface configuration command separately on each port. (CSCsi26392)

Device Manager Limitations

- When you are prompted to accept the security certificate and you click *No*, you only see a blank screen, and the device manager does not launch.

  The workaround is to click *Yes* when you are prompted to accept the certificate. (CSCef45718)

Important Notes

These sections describe the important notes related to this software release for the Catalyst 2960-S switches:

Switch Stack Notes

- Always power off a switch before adding or removing it from a switch stack.

Cisco IOS Notes

- You can only use the **logging on** and then the **no logging console** global configuration commands to disable logging to the console. (CSCec71490)
- If the switch requests information from the Cisco Secure Access Control Server (ACS) and the message exchange times out because the server does not respond, a message similar to this appears:

  ```
  00:02:57: %RADIUS-4-RADIUS_DEAD: RADIUS server 172.20.246.206:1645,1646 is not
  responding.
  ```

  If this message appears, check that there is network connectivity between the switch and the ACS. You should also check that the switch has been properly configured as an AAA client on the ACS

Device Manager Notes

- We recommend this browser setting to speed up the time needed to display the device manager from Microsoft Internet Explorer.

  From Microsoft Internet Explorer:

  1. Choose **Tools > Internet Options**.
  2. Click **Settings** in the "Temporary Internet files" area.
  3. From the Settings window, choose **Automatically**.
  4. Click **OK**.
  5. Click **OK** to exit the Internet Options window.
- If you use Internet Explorer Version 5.5 and select a URL with a nonstandard port at the end of the address (for example, *www.cisco.com:84*), you must enter *http://* as the URL prefix. Otherwise, you cannot launch the device manager.
- Japanese translation is available for the online help but not for the device manager GUI.
- When the switch is running a localized version of the device manager, the switch displays settings and status only in English letters. Input entries on the switch can only be in English letters.
- For device manager session on Internet Explorer, popup messages in Japanese or in simplified Chinese can appear as garbled text. These messages appear properly if your operating system is in Japanese or Chinese.
- You cannot create and manage switch clusters through the device manager. To create and manage switch clusters, use the CLI or Cisco Network Assistant.
- The HTTP server interface must be enabled to display the device manager. By default, the HTTP server is enabled on the switch. Use the **show running-config** privileged EXEC command to see if the HTTP server is enabled or disabled.

  If you are *not* using the default method of authentication (the enable password), you need to configure the HTTP server interface with the method of authentication used on the switch.

Beginning in privileged EXEC mode, follow these steps to configure the HTTP server interface:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**ip http authentication** {**aaa** | **enable** | **local**}	Configure the HTTP server interface for the type of authentication that you want to use. • **aaa**—Enable the authentication, authorization, and accounting feature. You must enter the **aaa new-model** interface configuration command for the **aaa** keyword to appear. • **enable**—Enable password, which is the default method of HTTP server user authentication, is used. • **local**—Local user database, as defined on the Cisco router or access server, is used.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show running-config**	Verify your entries.

The device manager uses the HTTP protocol (the default is port 80) and the default method of authentication (the enable password) to communicate with the switch through any of its Ethernet ports and to allow switch management from a standard web browser.

If you change the HTTP port, you must include the new port number when you enter the IP address in the browser **Location** or **Address** field (for example, http://10.1.126.45:184 where 184 is the new HTTP port number). You should write down the port number through which you are connected. Use care when changing the switch IP information.

Open Caveats

Unless otherwise noted, these severity 3 Cisco IOS configuration caveats apply to the Catalyst 2960-S switches:

- CSCsx7064

  When a switch stack is running 802.1x single host mode authentication and has filter-ID or per-user policy maps applied to an interface, these policies are removed if a master switchover occurs. Even though the output from the **show ip access-list** privileged EXEC command includes these ACLs, the policies are not applied.

  The workaround it to enter a **shutdown** and then a **no shutdown** interface configuration command on the interface.

- CSCsy85676

  When you configure an ACL and enter the **access-group** interface configuration command to apply it to an interface for web authentication, the output from the **show epm session ip-address** or **show ip access_list interface** *interface-id* privileged EXEC command does not show any web authentication filter ID.

  There is no workaround.

- CSCtc91312

  EnergyWise is enabled and you use the **energywise level** *level* **recurrence importance** *importance* **at** *minute hour day_of_month month day_of_week* interface configuration command to configure a recurring event on a switch. After the time changes from daylight savings time to standard time, the switch might

  – Restart when it tries to power a PoE device

  – Power on or off the PoE device at an incorrect time

  – Fail

  This occurs when the time change for the next year occurs after the time change for the current year.

  Before the time change occurs, use one of these workarounds:

  – Remove the recurring events from the EnergyWise configuration, do not use recurring events for a week, and reconfigure them a week after the time change occurs.

  – Use the **energywise level** *level* **recurrence importance** *importance* **time-range** *time-range-name* interface configuration command to reschedule the events.

  – Use the **power inline auto** interface configuration command to power on the PoE port.

- CSCte64832

  If you are downloading traffic from a 1000 Mb/s port to a 100 Mb/s port, congestion can occur and packets can be dropped.

  The workaround is to enable QoS, configure the ingress interface to trust CoS or trust DSCP, and increase the buffer size and weighted tail-drop (WTD) threshold level by 2000% or greater for the queue experiencing congestion.

Caution Take care when changing egress QoS configuration because the change affects multiple interfaces.

This example shows one way to increase the buffering capability of queue 4, threshold 3 in queue-set 1. The example assumes that QoS is enabled and that most traffic is best-effort traffic sent on queue 4, threshold 3.

```
Switch(config)# mls qos queue-setoutput 1 buffers 5 20 5 70
Switch(config)# mls qos queue-set output 1 threshold 4 200 200 100 2000
```

- CSCtf28627

  When you add 4000 VLAN instances to a switch that functions as a VLAN Trunking Protocol version 3 (VTPv3) server, memory fragmentation can occur and cause the switch to fail.

  Workaround: Do not configure more than 255 VLANs on a Cisco Catalyst 2960-S switch that functions as a VTPv3 server.

Documentation Updates

Update for the Catalyst 2960-S Hardware Installation Guide

The Catalyst 2960S-48TS-S and 2960S-24TS-S switches support the GLC-ZX-SM SFP module.

Related Documentation

These documents provide complete information about the switch and are available from this Cisco.com site:

http://www.cisco.com/en/US/products/ps6406/tsd_products_support_series_home.html

Note Before installing, configuring, or upgrading the switch, see these documents:

- For initial configuration information, see the "Using Express Setup" section in the getting started guide or the "Configuring the Switch with the CLI-Based Setup Program" appendix in the hardware installation guide.
- For device manager requirements, see the "System Requirements" section in the release notes (not orderable but available on Cisco.com).
- For Network Assistant requirements, see the *Getting Started with Cisco Network Assistant* (not orderable but available on Cisco.com).
- For cluster requirements, see the *Release Notes for Cisco Network Assistant* (not orderable but available on Cisco.com).
- For upgrading information, see the "Downloading Software" section in the release notes.

- *Release Notes for the Catalyst 2960-S Switches*
- *Catalyst 2960-S Switch Getting Started Guide*
- *Catalyst 2960 and 2960-S Switch Software Configuration Guide*
- *Catalyst 2960 and 2960-S Switch Command Reference*
- *Catalyst 3750, 3560, 3550, 2975, 2975, 2970, and 2960 and 2960-S Switch System Message Guide*
- *Catalyst 2960-S Switch Hardware Installation Guide*
- *Regulatory Compliance and Safety Information for the Catalyst 2960 and 2960-S Switches*
- *Release Notes for Cisco Network Assistant*
- *Getting Started with Cisco Network Assistant*
- *Cisco Redundant Power System 2300 Hardware Installation Guide*
- For more information about the Network Admission Control (NAC) features, see the *Network Admission Control Software Configuration Guide.*
- Information about Cisco SFP, SFP+, and GBIC modules is available from this Cisco.com site:

  http://www.cisco.com/en/US/products/hw/modules/ps5455/prod_installation_guides_list.html

  SFP compatibility matrix documents are available from this Cisco.com site:

  http://www.cisco.com/en/US/products/hw/modules/ps5455/products_device_support_tables_list.html

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.
